Task 10: Firewall Configuration Report

Name: Mohammed Fadil PK **Date:** January 30, 2026

1. Objective

The goal of this task was to secure a Linux system by configuring **UFW (Uncomplicated Firewall)**. I implemented a "Default Deny" policy and created specific rules to allow legitimate traffic while blocking malicious sources.

2. Installation & Initial Status

I first updated the repository and installed UFW on the Kali Linux machine. Initially, the firewall status was inactive, meaning the system was completely exposed to network traffic.

Fig 1: Status Inactive

3. Configuration & Rules Implemented

I applied the following security policies to harden the system:

- **Default Policies (Zero Trust):**
    - Incoming: Deny (Blocks all connections by default).
    - Outgoing: Allow (Allows the system to access the internet).
- **Service Access:**
    - **Port 22 (SSH):** Allowed to enable remote administration.
    - **Port 80 (HTTP):** Allowed for web server traffic.
- **Threat Blocking:**
    - **IP Ban:** Explicitly blocked traffic from the suspicious IP 192.168.1.50 to simulate mitigating an active attack.

4. Final Status Verification

After enabling the firewall, I verified the active rules using sudo ufw status verbose. The output confirmed that the policies were active and enforcing the rules as intended.

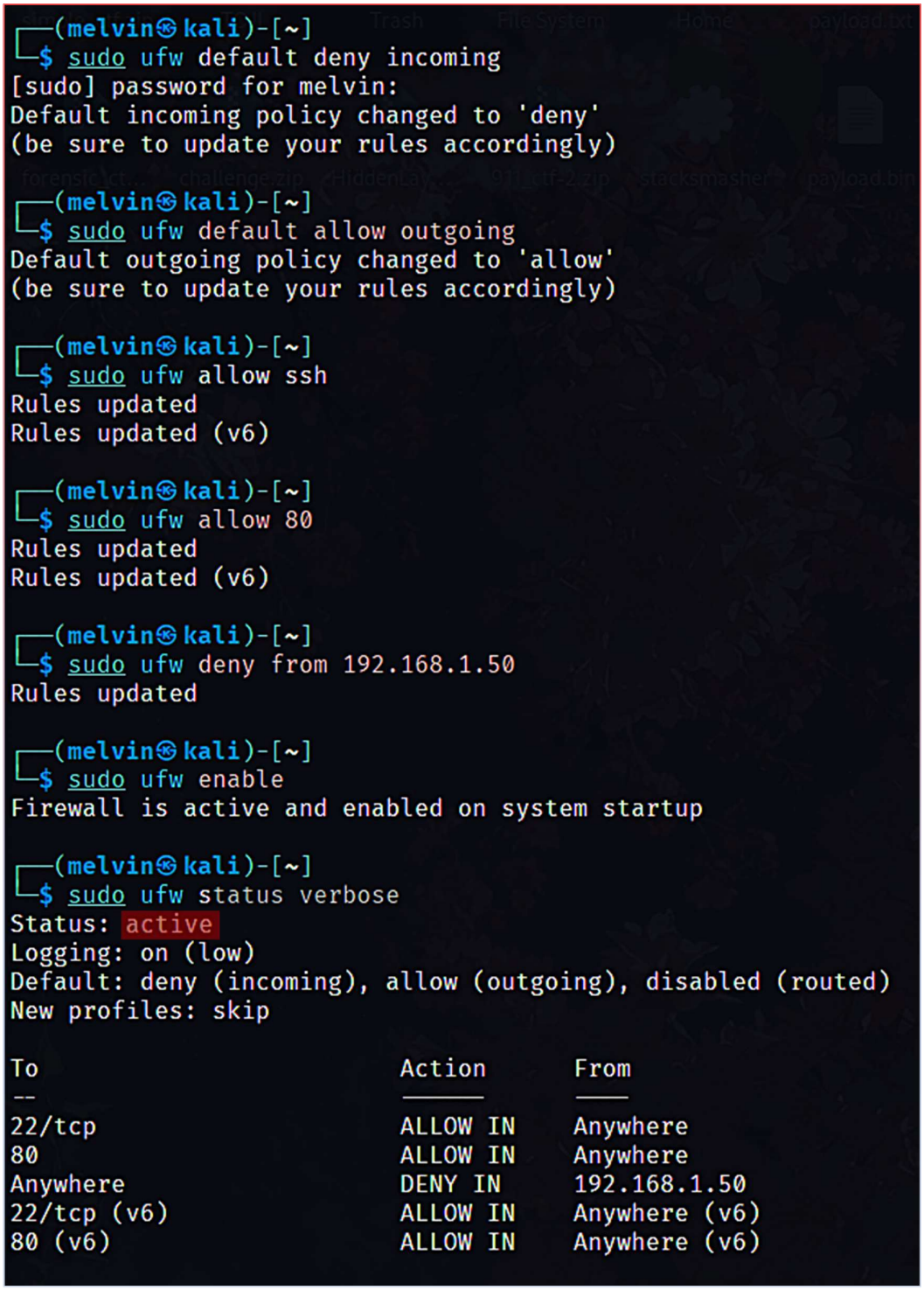

Fig 2: Status Active

5. Interview Questions & Answers

- **What is a Firewall?** A firewall is a network security device (hardware or software) that monitors and filters incoming and outgoing network traffic based on an organisation's previously established security policies. It acts as a barrier between a trusted internal network and untrusted external networks (like the Internet).
- **Stateful vs. Stateless Firewall?**
    - **Stateless:** Filters packets based only on the source, destination, and port, without tracking the "state" of the connection.
    - **Stateful:** Tracks the entire state of active network connections (e.g., TCP streams) and makes decisions based on the context of the traffic, not just individual packets.
- **Why are firewalls needed?** They prevent unauthorised access, block malicious traffic (like malware or DoS attacks), and ensure that only legitimate communication is allowed in and out of the network.
- **What is an Inbound vs. Outbound rule?**
    - **Inbound:** Controls traffic coming *into* the server (e.g., blocking hackers from connecting).
    - **Outbound:** Controls traffic going *out* of the server (e.g., preventing malware from sending stolen data to a C&C server).
- **Can a firewall stop all attacks?** No. Firewalls manage traffic flow but cannot stop attacks that happen *inside* allowed traffic (like SQL Injection or Phishing emails). They are just one layer of defence.

6. Conclusion

In this task, I successfully demonstrated how to manage network traffic using UFW. By setting a default "deny" policy and only opening necessary ports, I reduced the attack surface of the system. This exercise reinforced the importance of the "Least Privilege" principle in network security.